

## CLAIMS

- 1        1.        A computer controlled method comprising:  
2                    establishing communication between a provisioning device and a network  
3                    device over a preferred channel;  
4                    exchanging key commitment information over said preferred channel between  
5                    said provisioning device and said network device to pre-authenticate said network  
6                    device; and  
7                    providing provisioning information to said network device over said preferred  
8                    channel, whereby said network device can automatically configure itself for  
9                    communication over a network responsive to said provisioning information.
- 1        2.        The computer controlled method of claim 1, wherein said provisioning information  
2                    comprises network configuration information.
- 1        3.        The computer controlled method of claim 1, further comprising  
2                    receiving a public key from said network device;  
3                    verifying said public key with said key commitment information; and  
4                    automatically provisioning said network device with a credential authorized by  
5                    a credential issuing authority.
- 1        4.        The computer controlled method of claim 3, further comprising establishing proof  
2                    that said network device is in possession of a private key corresponding to said  
3                    public key.
- 1        5.        The computer controlled method of claim 3, wherein said credential issuing  
2                    authority is a certification authority and said credential is a public key certificate.

- 1 6. The computer controlled method of claim 3, wherein the step of automatically  
2 provisioning is responsive to authorization from a registration agent.
- 1 7. The computer controlled method of claim 1, wherein said preferred channel is a  
2 location-limited channel.
- 1 8. The computer controlled method of claim 1, wherein said preferred channel has a  
2 demonstrative identification property and an authenticity property.
- 1 9. The computer controlled method of claim 1, wherein the network is a wireless  
2 network, and wherein said provisioning device is a wireless access point.
- 1 10. The computer controlled method of claim 9, further comprising:  
2 receiving a wireless communication;  
3 determining whether said wireless communication originated from said  
4 network device or from a second network device that was not provisioned by said  
5 wireless access point; and  
6 routing said wireless communication responsive to the step of determining.
- 1 11. The computer controlled method of claim 10, wherein the step of routing  
2 comprises:  
3 choosing a selected channel from a secure channel and an insecure channel  
4 responsive to the step of determining; and  
5 sending said wireless communication through said selected channel.
- 1 12. The computer controlled method of claim 1, wherein said provisioning device is in  
2 communication with a credential issuing authority.
- 1 13. A computer-readable storage medium storing instructions that when executed by a  
2 computer cause the computer to perform a method to provision a network device,  
3 the method comprising steps of:

4 establishing communication between a provisioning device and said network  
5 device over a preferred channel;

6 exchanging key commitment information over said preferred channel between  
7 said provisioning device and said network device to pre-authenticate said network  
8 device; and

9 providing provisioning information to said network device over said preferred  
10 channel, whereby said network device can automatically configure itself for  
11 communication over a network responsive to said provisioning information.

1 14. The computer-readable storage medium of claim 13, further comprising

2 receiving a public key from said network device;

3 verifying said public key with said key commitment information; and

4 automatically provisioning said network device with a credential authorized by  
5 a credential issuing authority.

1 15. The computer-readable storage medium of claim 13, wherein the network is a  
2 wireless network, and wherein said provisioning device is a wireless access point.

1 16. An apparatus for provisioning a network device comprising:

2 at least one port configured to establish a preferred channel;

3 a preferred communication mechanism configured to be able to establish  
4 communication with and said network device over said preferred channel;

5 a pre-authentication mechanism configured to be able to receive key  
6 commitment information over said preferred channel from said network device; and

7 a provisioning mechanism configured to be able to provide provisioning  
8 information to said network device over said preferred channel, whereby said

- 9 network device can automatically configure itself for communication over a  
10 network responsive to said provisioning information.
- 1 17. The apparatus of claim 16, wherein said provisioning information comprises  
2 network configuration information.
- 1 18. The apparatus of claim 16, further comprising  
2 a key reception mechanism configured to receive a public key;  
3 a key verification mechanism configured to verify said public key with said  
4 key commitment information; and  
5 a credential provisioning mechanism configured to automatically provide a  
6 credential authorized by a credential issuing authority.
- 1 19. The apparatus of claim 18, further comprising a key exchange mechanism  
2 configured to be able to perform a key exchange protocol with said network device.
- 1 20. The apparatus of claim 18, wherein said credential issuing authority is a  
2 certification authority and said credential is a public key certificate.
- 1 21. The apparatus of claim 16, wherein said preferred channel is a location-limited  
2 channel.
- 1 22. The apparatus of claim 16, wherein the network is a wireless network, and the  
2 apparatus further comprises a wireless access point mechanism.
- 1 23. The apparatus of claim 22, further comprising:  
2 a packet receiver mechanism configured to receive a wireless communication;  
3 a determination mechanism configured to determine whether said wireless  
4 communication received by the packet receiver mechanism originated from said  
5 network device or from a second network device that was not provisioned by said  
6 wireless access point; and

7           a router mechanism configured to route said wireless communication  
8 responsive to the determination mechanism.

1       24.   The apparatus of claim 23, wherein the router mechanism further comprises:

2           a channel selection mechanism configured to choose a selected channel from a  
3 secure channel and an insecure channel responsive to the determination mechanism;  
4 and

5           a transmission mechanism configured to send said wireless communication  
6 through said selected channel.

1       25.   The apparatus of claim 16, further comprising a non-preferred communication  
2 mechanism that can be used to communicate with a credential issuing authority.

1       26.   A computer controlled method comprising:

2           establishing communication between a network device and a provisioning  
3 device over a preferred channel;

4           receiving provisioning information from said provisioning device over said  
5 preferred channel;

6           exchanging key commitment information over said preferred channel between  
7 said provisioning device and said network device to pre-authenticate said network  
8 device; and

9           automatically configuring said network device for communication over a  
10 network responsive to said provisioning information.

1       27.   The computer controlled method of claim 26, further comprising executing a key  
2 exchange protocol.

- 1 28. The computer controlled method of claim 27, further comprising establishing a  
2 communication channel between said network device and a credential issuing  
3 authority responsive to the step of executing wherein said communication channel  
4 is secure.
- 1 29. The computer controlled method of claim 26, wherein the network is a wireless  
2 network, said provisioning device is a wireless access point, and wherein said  
3 provisioning information comprises a service set identifier (SSID).
- 1 30. The computer controlled method of claim 29, wherein the network is a wireless  
2 network, said provisioning device is a wireless access point, and wherein said  
3 provisioning information comprises a privacy key.
- 1 31. The computer controlled method of claim 26, wherein said provisioning  
2 information comprises a credential.
- 1 32. The computer controlled method of claim 26, further comprising  
2 receiving a public key from said provisioning device;  
3 verifying said public key with said key commitment information; and  
4 automatically provisioning said network device with a credential authorized by  
5 a credential issuing authority.
- 1 33. The computer controlled method of claim 32, wherein the network is a wireless  
2 network, said provisioning device is a wireless access point, and wherein said  
3 provisioning information comprises a service set identifier (SSID).
- 1 34. The computer controlled method of claim 33, wherein the network is a wireless  
2 network, said provisioning device is a wireless access point, and wherein said  
3 provisioning information comprises a privacy key.
- 1 35. The computer controlled method of claim 32, wherein said provisioning  
2 information comprises network configuration information.

- 1 36. The computer controlled method of claim 32, wherein the step of automatically  
2 provisioning is responsive to authorization from a registration agent.
- 1 37. The computer controlled method of claim 32, wherein said credential issuing  
2 authority is a certification authority and said credential is a public key certificate.
- 1 38. The computer controlled method of claim 26, wherein said preferred channel is a  
2 location-limited channel.
- 1 39. The computer controlled method of claim 26, wherein said preferred channel has a  
2 demonstrative identification property and an authenticity property.
- 1 40. The computer controlled method of claim 26, wherein said network device is from  
2 one or more of the group consisting of a computer, a personal data assistant, a smart  
3 card, a cryptographic token, a medical device, a device containing personal  
4 information, a secure telephone, a cell telephone, a vehicle, a container, an access  
5 card, a biometric sensor, a wireless network device, a proximity sensor, a sensor  
6 device, traffic sensor, an alarm device, a robot, a device capable of receiving a  
7 credential, a device capable of issuing a credential.
- 1 41. A computer-readable storage medium storing instructions that when executed by a  
2 computer cause the computer to perform a method to automatically provision a  
3 network device, the method comprising steps of:  
4 establishing communication between said network device and a provisioning  
5 device over a preferred channel;  
6 receiving provisioning information from said provisioning device over said  
7 preferred channel;  
8 exchanging key commitment information over said preferred channel between  
9 said provisioning device and said network device to pre-authenticate said network  
10 device; and

11                    automatically configuring said network device for communication over a  
12                    network responsive to said provisioning information.

1        42.        The computer-readable storage medium of claim 41, wherein said preferred channel  
2                    has a demonstrative identification property and an authenticity property.

1        43.        The computer-readable storage medium of claim 41, wherein said network device is  
2                    from one or more of the group consisting of a computer, a personal data assistant, a  
3                    smart card, a cryptographic token, a medical device, a device containing personal  
4                    information, a secure telephone, a cell telephone, a vehicle, a container, an access  
5                    card, a biometric sensor, a wireless network device, a proximity sensor, a sensor  
6                    device, traffic sensor, an alarm device, a robot, a device capable of receiving a  
7                    credential, a device capable of issuing a credential.

1        44.        An apparatus comprising:  
2                    at least one port configured to establish a preferred channel;  
3                    a preferred channel communication mechanism configured to be able to  
4                    establish communication with a provisioning device over said preferred channel;  
5                    a receiver mechanism configured to be able to receive provisioning  
6                    information from said provisioning device over said preferred channel;  
7                    a pre-authentication mechanism configured to be able to receive key  
8                    commitment information over said preferred channel from said provisioning  
9                    device; and

10                    a communication setup mechanism configured to automatically configure the  
11                    apparatus for communication over a network responsive to said provisioning  
12                    information received by the receiver mechanism.

1        45.        The apparatus of claim 44, wherein said provisioning information comprises  
2                    network configuration information.



- 1 46. The apparatus of claim 44, wherein the network is a wireless network, said  
2 provisioning device is a wireless access point, and wherein said provisioning  
3 information comprises a service set identifier (SSID).
- 1 47. The apparatus of claim 44, wherein said provisioning information comprises a  
2 credential.
- 1 48. The apparatus of claim 44, further comprising a key exchange mechanism  
2 configured to execute a key exchange protocol.
- 1 49. The apparatus of claim 44, further comprising  
2 a key reception mechanism configured to receive a public key;  
3 a key verification mechanism configured to verify said public key with said  
4 key commitment information; and  
5 a credential receiver mechanism configured to receive a credential authorized  
6 by a credential issuing authority.
- 1 50. The apparatus of claim 49, wherein the credential receiver mechanism is capable of  
2 being responsive to authorization from a registration agent.
- 1 51. The apparatus of claim 49, wherein the network is a wireless network, said  
2 provisioning device is a wireless access point, and wherein said provisioning  
3 information comprises a service set identifier (SSID).
- 1 52. The apparatus of claim 51, wherein the network is a wireless network, said  
2 provisioning device is a wireless access point, and wherein said provisioning  
3 information comprises a privacy key.
- 1 53. The apparatus of claim 49, wherein said credential issuing authority is a  
2 certification authority and said credential is a public key certificate.

1 54. The apparatus of claim 44, wherein said preferred channel is a location-limited  
2 channel.

1 55. The apparatus of claim 44, wherein the apparatus is from one or more of the group  
2 consisting of a computer, a personal data assistant, a smart card, a cryptographic  
3 token, a medical device, a device containing personal information, a secure  
4 telephone, a cell telephone, a vehicle, a container, an access card, a biometric  
5 sensor, a wireless network device, a proximity sensor, a sensor device, traffic  
6 sensor, an alarm device, a robot, a device capable of receiving a credential, a device  
7 capable of issuing a credential.